BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04K 1/00

A1

(11) International Publication Number: WO 99/46881

(43) International Publication Date: 16 September 1999 (16.09.99)

(21) International Application Number: PCT/IL98/00116

(22) International Filing Date: 11 March 1998 (11.03.98)

(71) Applicant *(for all designated States except US)*: GUARDTECH TECHNOLOGIES LTD. [IL/IL]; Tozeret Ha'aretz Street 16, 67891 Tel Aviv (IL).

(72) Inventor; and

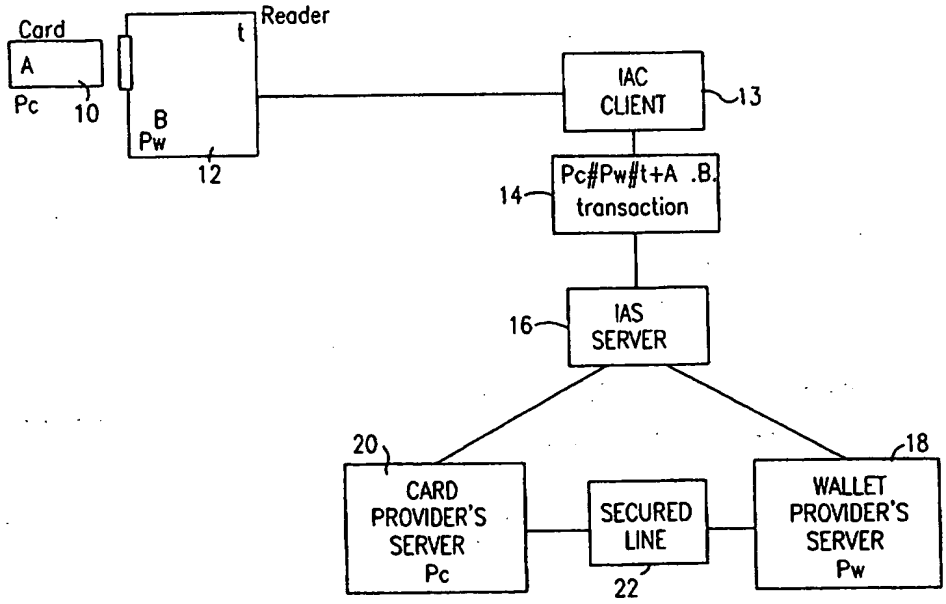
(75) Inventor/Applicant *(for US only)*: RASHMAN, Ziv [IL/IL]; Hashoftim Street 52, 47210 Ramat Hasharon (IL).

(74) Agents: COLB, Sanford, T. et al.; Sanford T. Colb & Co., P.O. Box 2273, 76122 Rehovot (IL).

(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: TRANSACTION CARD SECURITY SYSTEM



(57) Abstract

User verification for transactions in which the user has a transaction card (10) and his own card reader (12) is provided by assigning to the card and the reader both a public and a secret number. A one-way encoding function is used to encode the secret numbers, and the public numbers are used at the provider end to elicit corresponding secret numbers from separately located databases (18, 20). The corresponding secret numbers are encoded using the same one-way function at the provider end and if the result is the same as that performed at the sending end then the user is positively identified. The two databases are kept apart so that no single location can be hacked into to reveal enough information for the system to be successfully abused.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Transaction Card Security System

Field Of The Invention

The present invention relates to security systems for transaction cards, including smart cards and magnetic strip cards.

Background Of The Invention

Transaction cards are widely used for making purchases and for obtaining cash and credit, and it has long been a preoccupation with card providers to provide security against theft for such cards. Recently there has been a growing tendency to use cards of this type in transactions made over the telephone or the internet or like unsecured public networks. In many cases transactions over the telephone are made verbally and involve the card owner reading out the serial number printed on the card. In other cases transactions over the telephone are carried out using the numerical keys of the telephone, a computer at the receiving end being adapted to recognize the tones associated with each numerical key. In neither case is any security provided, and the card holder is vulnerable should anyone be eavesdropping on the communication. However in such transactions no security is possible because the transaction is made directly between the two parties and thus no secret information can be used.

It is therefore desirable to use a system of authorizing transactions between two parties, whether made over the telephone, or the internet or like unsecured public communication network, or whether made face to face in a shop or the like, that allows the use of secret information to authorize the transaction, without handing over any secret information to the other party to the transaction or for that matter to eavesdroppers on the public communication network.

It has been proposed to provide each cardholder, or group of cardholders, with an electronic card reader that is portable and can be plugged in to the relevant communications network. The transaction card is entered into a receiving port and the

card reader has a keyboard and screen so that the user PIN associated with the card can be entered. The card reader then encodes the pin and sends the encoded PIN together with details of the transaction to a server associated with the provider of the card, who authorizes the transaction. The card reader is a small, waferlike device, of about the thickness of three of the transaction cards and contains a central processor and memory as well as a connector for connecting the device to a communications network.

In an improvement of the above proposal the card reader is issued with a serial number. The serial number is transmitted with the transaction information and part of the authorization procedure involves matching up the card reader with the card. If the card is authorized to be used with that reader then the transaction is allowed and if not then the transaction is not authorized.

Thus the serial number of the reader is used for identification purposes. However the only secret information that is used in the authorization process is the PIN associated with the card. This number must be kept short because it has to be memorized by the user, usually four digits is the maximum length, and therefore the total amount of secret information that is used to establish the transaction is not that great. Furthermore, no secure system is used to establish the identity of the card reader.

A recent development in the use of transaction cards is the EP protocol for electronic money. A secure file is 'minted' as the electronic coin and is loaded onto the card. The coin is used in transactions involving the card and the card holder would wish to be able to use his coins securely without having to impart his secret information to equipment belonging to the other party to the transaction. The protocols involving electronic money require considerable processing power and therefore a card reader at least of the type described above is needed. Furthermore a means is needed to allow the card holder to manage his electronic money as electronic coins cannot be removed from a wallet and counted.

Summary of the Invention

An object of the present invention is to provide a system by which both the card and reader can be separately identified, and in respect of which no single computer has stored therein sufficient information to carry out the identification itself.

It is a further object of the present invention to ensure that secret information placed on an insecure public communications network to enable the above mentioned identification operation cannot be decrypted to allow discovery of the secret information with any significant degree of certainty.

It is yet a further object of the present invention to provide a system by which the total amount of secret information involved in the identification procedure exceeds the length of a password or PIN that the cardholder can reasonably be expected to remember.

Various embodiments of the present invention fulfill one or more of the above objects.

According to a first aspect of the present invention there is provided a system for identifying users, having user-end apparatus and provider end apparatus.

Each user-end apparatus comprises a first part having a public key and a secret key and a second part having a public key and a secret key, an encrypter for encrypting said two secret keys together using a one-way function, and an output for transmitting said public keys, said encrypted secret keys and other data.

The provider end apparatus comprises two separately located databases, one matching public and secret keys of first parts of said user-end apparatus and the second matching public and secret keys of second parts, a selector at each database to select secret keys corresponding to the public keys of each part, an encrypter for encrypting secret keys found on said data bases, a comparator to compare the result of the

encryption at the provider end apparatus with the result of the encryption produced at the user-end apparatus, and an output for signaling the result of the comparison to indicate whether the user has been successfully identified.

In an embodiment the provider end apparatus has a third database matching public keys of said first and second parts of said user end apparatus, and wherein said third database is operated by control electronics to inhibit successful identification of said user unless said third database indicates a match between said two public keys..

The comparator is preferably located together with one of said separately located databases, and said secret key selected at the other of said separately located databases is sent to said comparator via a secure communication means.

The first part of said user-end apparatus may be any of a smart card and a magnetic strip card, and said second part of said user-end apparatus may be a portable card reader assigned to a user.

The secret key of said first part of said user-end apparatus is preferably not recorded on said first part. Rather it is a secret pin number memorised by the user.

The secret key of said second part of said user end apparatus may be variable in accordance with a variation procedure. In such an embodiment the variation procedure is preferably not recorded on said second part.

In order to form an authentication signature the encrypters may be operable to encrypt said secret key of said first part, said secret key of said second part and perhaps also a time varying element. Other elements may be optionally included.

The encryption may be carried out using a one-way hashing function.

The user end apparatus may be connected to a transaction target, and said transaction target is adapted to receive from said user end apparatus one or more of the public keys, transaction data and said encrypted secret keys, and to relay said at least the same to said provider end apparatus via a, public communication network, and to receive said acknowledgment output from said provider end apparatus. The transaction target may add its own identification data, either secret or public, for verifying by the provider end apparatus.

According to a second aspect of the present invention there is provided a method of identifying a user comprising,

supplying a user with a first identification part having a public and a secret key and a second identification part having a public and a secret key,

encrypting together said secret key of said first part and said secret key of said second part using a one-way encryption function to form a first encryption result,

transmitting said public keys and the result of said encryption step to a verification apparatus,

transmitting said public key of said first part to a database that matches public and secret keys of said first part and finding a corresponding secret key,

transmitting said public key of said second part to a database that matches public and secret keys of said second part and finding a corresponding secret key,

encrypting together said secret keys obtained from said databases using said one-way encryption function to form a second encryption result,

comparing said first and second encryption results and, if they are identical, then indicating successful identification of said user.

Brief Description Of The Drawings

For a better understanding of the invention and to show how the same may be carried into effect, reference will now be made, purely by way of example, to the accompanying drawings in which,

Figure 1shows a first embodiment of the invention,

Figure 2 shows a part of figure 1 in more detail,

Figure 3 shows a second embodiment of the invention,

Figure 4 shows a third embodiment of the invention, and

Figure 5 shows a fourth embodiment of the present invention.

Description Of The Preferred Embodiments

Figure 1 shows a first embodiment of the invention. A card 10 is provided to the user and may preferably be a smart card or a magnetic card and may contain identification data A. Identification data A is stored on the card, either in an electronic memory or on the magnetic strip. This data is not regarded as especially secure as it can be read by a card reader. Associated with the card is a user secret number or pin number P_s which is not recorded on the card and is known only to the user and to the provider of the card.

The user is also provided with a card reader 12. The card reader 12 is preferably a small portable device unique to the user. An example of the device 12 is shown in greater detail in figure 2 and comprises card reader apparatus 30, a small keyboard 32, a small LCD screen 34, a memory 36, some signal processing ability 38 and an output port 40. A power supply 40 may preferably be a battery, and recharging means may be included. All of these may be controlled by a processor 44. The card reader apparatus 30 may preferably include a reader for a magnetic strip and a reader for a smart card. The output means may simply be a tone generator that generates DTMF tones in accordance with numbers to be sent, and may thus work by placing the device next to the telephone speaker in order to effect transmission. In other embodiments the output means may be a generator of digital signals for use in an internet connection. The output may also be designed to be connected directly to transaction equipment 13 belonging to a vendor.

The output is connected to a secret data memory 46 and the memory 36 only via the processor 44 which carries out the encryption, so that there is no possibility of secret information being sent out unencrypted from the card reader apparatus. The purpose of the card reader is to enable the user to use secret data to validate a transaction made through apparatus such as transaction equipment 13 in the possession of a third party, without at the same time handing over the secret data to the third party.

The card reader may have identification data B and may also have a secret number P_w which is stored inside the machine and is known only to the issuer of the card reader. Identification data B may be stored in the machine 12 or may be a password typed in by the user. The card reader 12 is designed to be connected via output port 40, to a communications network such as the public telephone network or the internet or, as shown in figure 1, directly to transaction apparatus of a third party. Neither the transaction apparatus nor the communications network can be regarded as secure and therefore any sensitive data to be transferred must be encrypted. The card reader 12 is therefore able to encrypt data using a one way function. In a preferred embodiment the one way function is a hashing function. A hashing function is a function that is many to one, that is to say more than one input can lead to a given output. Hence the function is one way, that is to say there is no inverse function that will allow the input to be derived unambiguously from the output. In an embodiment a group of one-way hashing functions known as MD5 is used.

In order to carry out a transaction using the card and the reader, all that is necessary is for the user to insert the card 10 into the reader 12 and type in the pin number, as well as any relevant details of the transaction. The reader 12 is connected via the output port 40, and it calculates the hashing product of say the pin code P_c and the secret number of the reader P_w, as well as of a third component that varies over time, for example the output of clock 46. A time varying component is preferred so that the eavesdropper cannot simply copy the encrypted message and make it appear that he has access to the secret numbers when he does not.

The result of the hashing operation is sent as an authentication signature. The remainder of the details of the transaction, including identification data of the card A and of the reader B, are sent unencrypted. Alternatively they are sent encrypted using a scheme that allows their decryption at the far end, for example a DES (data encryption standard) scheme.

The entire transmission relating to the transaction is preferably received by an IAS client 13, which is a computerised transaction apparatus belonging to the other party to the transaction. The client validates certain details of the transaction such as value and time, perhaps compares the username with a private list of bad debtors or the like, and then adds its own ID code C to the transaction transmission. The transmission is then sent via a communication network 14 to an IAS (Identification and Authorization Server) 16. The communication network may, for example, be the public telephone network or the Internet.

The server first identifies the IAS client using using the identification data C. Then it identifies at least enough information from the unencrypted part of the data to select appropriate destinations to pass on the information. That is to say it determines who the card provider is and who has provided the reader. The authentication signature is thus directed to a server 20 which belongs to the provider of the card. This transmission may be made over an insecure data connection.

The server 20 sends on the reader public number B to a server 18 belonging to the appropriate provider of card readers. The server 18 is able to identify which card reader 12 is involved in the transaction from the identification data B. It is therefore able to supply the secret number of the card reader p_w. The authentication signature plus P_w are sent over a secure communication link 22 to the server 20. The card provider knows from the card identification data A which card is being used and is therefore able to provide the corresponding pin or secret number P_c. The time of the transaction is known because it is approximately the same as that of a clock at the server 20. Alternatively the time may be transmitted unencoded as well as within the signature. The card server thus

has all of the components that went into the signature and it repeats the hashing function with the components it has obtained independently. If this produces the same result as the signature, and provided that the card is authorized for use with that same card reader, then the transaction is authorized and a signal to this effect is transmitted to the IAS server 16.

The transaction may now be completed by signalling authorisation of the transaction to the IAS client. The secret number of the card reader P_w is not stored in the server 20 once the authorization is completed. For the short period until the verification is completed it is preferably stored only in volatile memory as part of a data structure that is protected from being copied by the operating system into non-volatile memory even as a temporary swap file. Thus no single server has the ability to authenticate the signature and there is no single server that can be tapped illegally to obtain enough information to forge a signature. Furthermore even the tapping of secure communication link 22 would not enable the user to obtain enough information to forge a signature.

It will be appreciated by the person skilled in the art that either of the two servers 18 and 20 may carry out the authentication procedure, that is to say, either the card provider's server or the reader provider's server, may be sent the authentication signature, and carry out the authentication check. In a further variation the server that is not provided with the authentication signature may be provided directly with its respective public key from the IAS server 16 without the mediation of the the other server.

Figure 3 is a preferred embodiment operative in accordance with the present invention. In a transaction involving electronic money, the recipient may not have an IAS client. In these circumstances the tasks of the IAS client are carried out in association with the IAS server 16.

In an alternative embodiment the need to send a secret number over a secured network is avoided. As before, the encryption product and the public numbers are received at the IAS server. The public numbers are sent to their respective servers with the encryption product. The corresponding secret numbers are found at each server 18 and 20 and are separately encrypted at each server. Then the secured link 20 is used to send the encrypted version of one of the numbers to the other server which is then able to complete the identification as before, but without at any time having held the other secret number. The only additional requirement for this alternative embodiment is that the one-way function is commutative.

The card reader secret number P_w is preferably stored within the card reader as part of a secret data memory 46. The connections to the secret data memory 46 are such that there is no readout operation that enables the secret number to be accessed. That is to say it cannot be read out except via the circuits for the encrypting function. The secret data memory 46 is positioned within the card reader 12 in such a position that access is difficult and it is designed to wipe the information in the event of a direct attempt to access the data.

The secret number of the card reader could be a fixed code of fixed length. Its length is not restricted by the need for a user to be able to remember it as it is stored in the reader. Alternatively the length of the key could be varied in some way. For example the secret data memory 46 may store a matrix of information and use different parts of this matrix at different times in accordance with a predetermined algorithm. Thus the length and the content of the secret number may be changed as desired. This has the added advantage that there is no single part of the card reader that can be hacked to obtain the secret number. The algorithm for varying the number need not be stored anywhere within the card reader.

As a further alternative one of the secret numbers could be a number constructed in accordance with the recognition of the fingerprint of the user or some other invariant personal authentication means.

Instead of an output port that demands physical contact between the card reader and the terminal of the communication network, it is possible to make an output port that sends infra-red signals, the terminal of the communication network being operative to detect these signals and convert them into a form suitable for sending down the network.

In a more elaborate version, the card reader may produce two sets of authentication signatures, each based on different sets of public and secret information. For example the card may have two public numbers A and A', and the card reader may likewise have two sets of such numbers B and B' as well as two secret numbers P_w and P_w'. Each of the signatures may then be sent for authentication to different pairs of servers respectively.

The card itself is essentially a data storage device. Indeed a smart card can store many kilobytes of data. Thus the card reader, which is in fact not just a reader but a writer as well, can incorporate considerable data management abilities. It can be used to store databases on the card, as well as programs, and can be used to call programs from the card and run them. The keyboard 32 is available to the user to write directly to the card, allowing it to serve as a notebook, diary and address book as well as a credit card. The credit card reader 12 is also able to support the protocols necessary for EP standard electronic money and therefore the combination of card and reader serve as an electronic wallet.

As mentioned above, the secret numbers may be encrypted together with the time, which is generated in the clock 46 of the reader. Preferably the time used is GMT or some other agreed standard, so that international transactions are not adversely affected.

In the embodiments described above the use of a card has been restricted to given readers because the public numbers of the card and reader are checked against a third database that lists the cards authorized for use with each reader. Thus any abuser of the system is obliged to hack three databases in order to obtain sufficient information to

impersonate a user successfully. The three databases are preferably located on different machines at separate locations belonging to different organizations and arranged to prevent hacking.

It is possible to configure the system such that only transactions above a certain amount are restricted to a given reader/card combination and this is a way of striking a balance between convenience and security. As an additional level of security the reader may require a user-entered password, in addition to the PIN of the card, and may lock up, that is to say may cease to operate, after a given number of unsuccessful attempts to enter the password. Unlocking of the card is an operation that can only be carried out by an authorized maintenance center. It may depend on a further pin number, or any one of a range of alternative schemes well known to the skilled man.

Figure 4 is a simplified embodiment of the invention. In figure 4, parts that are the same as those shown in figure 1 or figure 3 are given identical reference numerals. In this figure neither a separate IAS client nor a separate IAS server are shown.

The card reader 12 has an encrypter 50 and the output 40 has the ability to route the transmission, including the encrypted portion thereof, directly to the two servers 18 and 20 that hold the databases of public against secret numbers. Each of the servers has a selector, 52 which selects the appropriate secret number for the received public number. In one of the servers 18 the secret number selected is sent via secure connection 22 to the other server 20 where it is placed in an encrypter 54. Encrypter 54 is identical in operation to that 50 in card reader 12. The secret number selected by selector 52 in server 20 is likewise placed in encrypter 54, and an encryption operation is carried out on the two secret numbers plus the same time varying element, for example the time, that is indicated as the time of the transaction by the unencoded information sent by the card reader.

The result of the encryption is passed to a comparator 56 where it is compared with the encoded information received directly from the card reader. If they are the same

then a transaction authorization signal is sent out, via output 58, to the public network. In a variation the secret number that is sent from server 18 to server 20 is sent encrypted for additional security, although in this case the encryption operation used is a reversible encryption operation as it is necessary to extract the secret number at server 20.

Figure 5 shows an embodiment of the invention for use in telephone based ordering or for orders made over the internet, and in which the order is received by the vendor using electronic means. A card reader with card inserted 60 is connected either directly to a telephone 62 or to an infra-red link terminal 64 or to a PC 66, which has itself been connected to the vendor 70 through the telephone network or the internet or like unsecured public network, 68. Vendor processing apparatus 72 sets up the transaction with the user, and, as the transaction is completed the vendor processing apparatus requests authentication from the purchaser. The purchaser types in his secret number P_c as before and the card reader/card combination sends an authentication signature.

The vendor processing apparatus receives the transmission but is unable to discover the purchaser's secret keys. The authentication signature is passed, together with identification data of the vendor 70, back to the public network 68 and thence to the IAS server 16 where it is processed as described previously. Thus the identity of a purchaser can be authenticated through the vendor's processing apparatus without the vendor being able to discover any secret information of the purchaser.

It will be appreciated that in each of the above embodiments one or other of the secret numbers P_c and P_w could be assigned a zero value. The system is operated in exactly the same way and may be used to provide independent identification for either the card or the reader.

In a further embodiment of the invention it is possible to encode the public number of the card. This is desirable in order to keep the public number from the vendor. At the present time it is possible to use credit cards solely on the strength of the public number, for example in telephone ordering. Because the public number has to be known in order

to identify the signature a two-way encription algorithm has to be used. The encryption of the public number is carried out using the reader 12, which contains an encryption key that can be used for a two-way encryption algorithm such as DES. The public number is decrypted by the IAS server 16, which now has all the information it needs to route the signature to the servers of the correct providers.

It is appreciated that the various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

Claims

1. A system for identifying users, comprising user-end apparatus and provider end apparatus,

wherein each user-end apparatus comprises a first part having a public number and a secret number and a second part having a public number and a secret number, an encrypter for encrypting said two secret numbers together using a one-way function, and an output for transmitting said public numbers, said encrypted secret numbers and other data,

wherein the provider end apparatus comprises two separately located databases, one matching public and secret numbers of first parts of said user-end apparatus and the second matching public and secret numbers of second parts, a selector at each database to select secret numbers corresponding to the public numbers of each part, an encrypter for encrypting secret numbers found on said data bases, a comparator to compare the result of the encryption at the provider end apparatus with the result of the encryption produced at the user-end apparatus, and an output for signaling the result of the comparison to indicate whether the user has been successfully identified.

2. A system according to claim 1 wherein said provider end apparatus has a third database matching public numbers of said first and second parts of said user end apparatus, and wherein said third database is operated by control electronics to inhibit successful identification of said user unless said third database indicates a match between said two public numbers..

3. A system according to claim 1 wherein said comparator is located together with one of said separately located databases, and said secret number selected at the other of said separately located databases is sent to said comparator via a secure communication means.

4. A system according to claim 1 wherein said first part of said user-end apparatus is one of a group comprising a smart card and a magnetic strip card, and said second part of said user-end apparatus is a portable card reader assigned to a user.

5. A system according to claim 4 wherein said secret number of said first part of said user-end apparatus is not recorded on said first part.

6. A system according to claim 4 wherein said secret number of said second part of said user end apparatus is variable in accordance with a variation procedure.

7. A system according to claim 6 wherein said variation procedure is not recorded on said second part.

8. A system according to claim 1 wherein said encrypters are operable to encrypt said secret number of said first part, said secret number of said second part and a time varying element.

9. A system according to claim 1 wherein said encrypters are operable to encrypt using a one-way hashing function.

10. A system according to claim 1 wherein said user end apparatus is connected to a transaction target, and said transaction target is adapted to receive from said user end apparatus at least one of a group comprising said public numbers, transaction data and said encrypted secret numbers, and to relay said at least one of said group to said provider end apparatus via a, public communication network, and to receive said acknowledgment output from said provider end apparatus.

11. A system according to any preceding claim wherein said public number of said first part is encrypted prior to transmission using a two-way encryption function.

12. A method of identifying a user comprising

supplying a user with a first identification part having a public and a secret number and a second identification part having a public and a secret number,

encrypting together said secret number of said first part and said secret number of said second part using a one-way encryption function to form a first encryption result,

transmitting said public numbers and the result of said encryption step to a verification apparatus,

transmitting said public number of said first part to a database that matches public and secret numbers of said first part and finding a corresponding secret number,

transmitting said public number of said second part to a database that matches public and secret numbers of said second part and finding a corresponding secret number,

encrypting together said secret numbers obtained from said databases using said one-way encryption function to form a second encryption result,

comparing said first and second encryption results and, if they are identical, then indicating successful identification of said user.

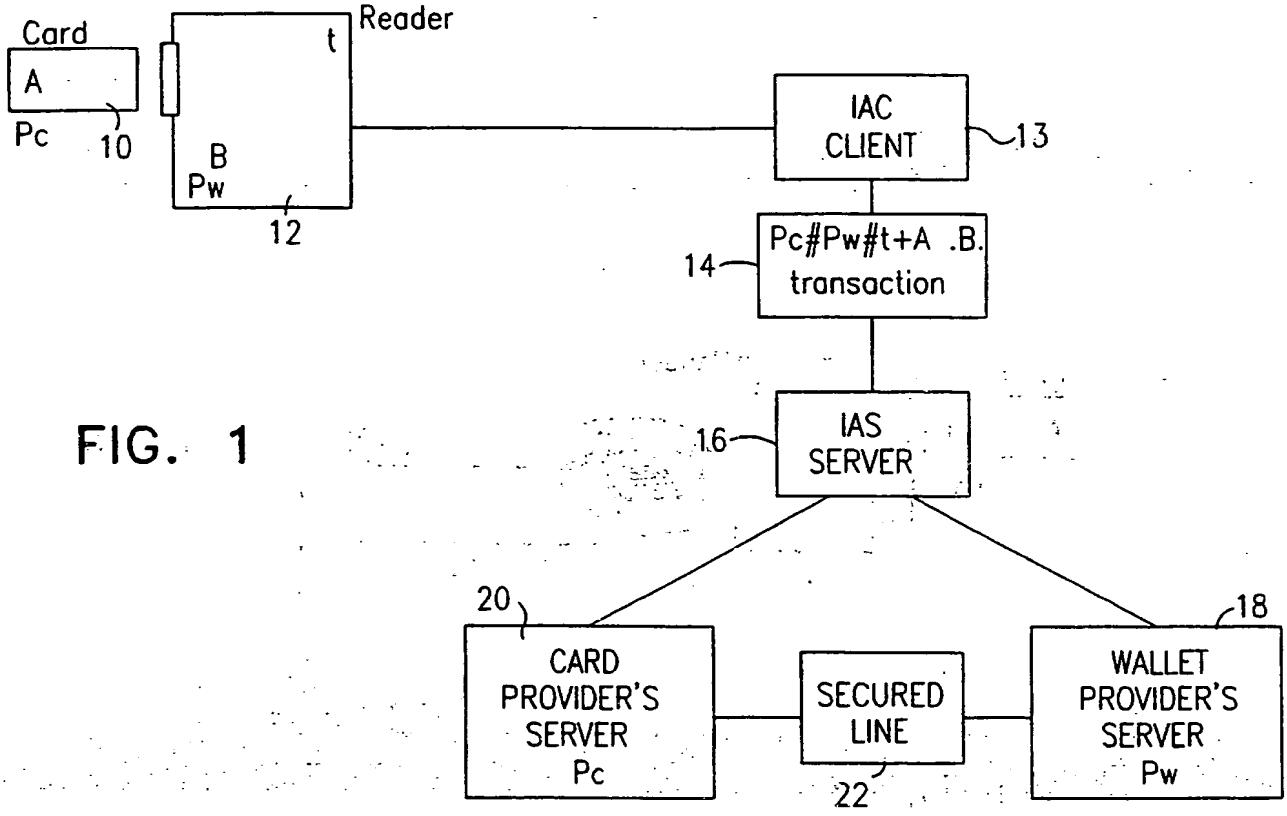
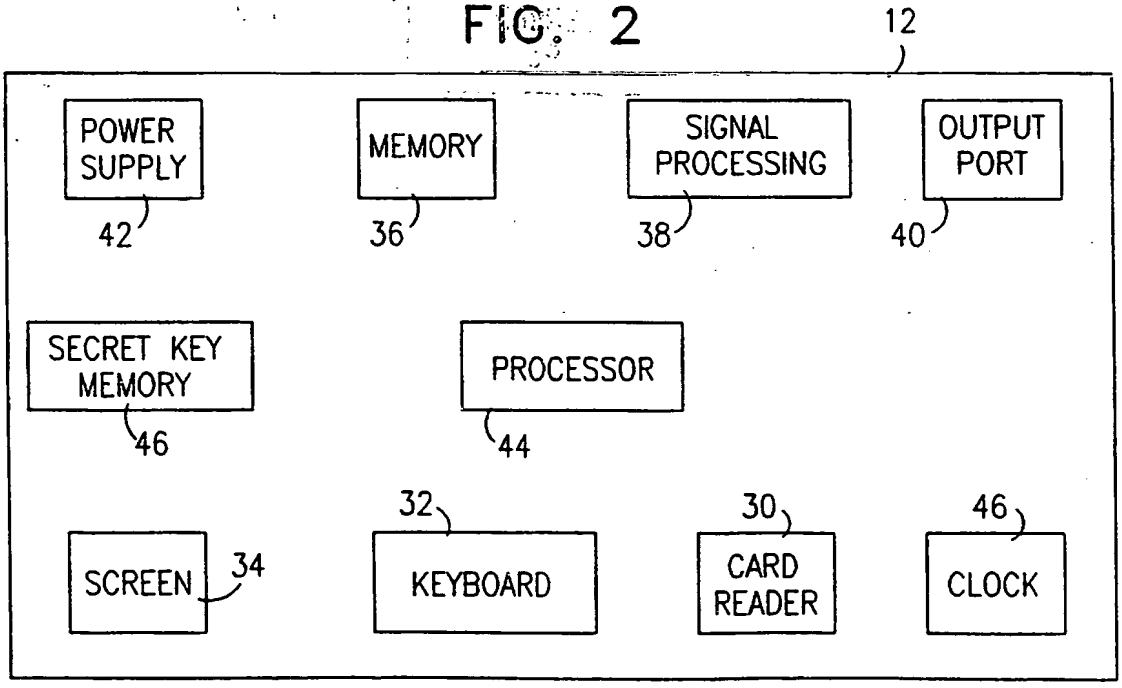

Card
A
Pc
10
Reader
t
B
Pw
12
IAC
CLIENT
13
Pc#Pw#t+A .B.
transaction
14
IAS
SERVER
16
20
CARD
PROVIDER'S
SERVER
Pc
SECURED
LINE
22
18
WALLET
PROVIDER'S
SERVER
Pw

FIG. 1

FIG. 2


12
POWER
SUPPLY
42
MEMORY
36
SIGNAL
PROCESSING
38
OUTPUT
PORT
40
SECRET KEY
MEMORY
46
PROCESSOR
44
32
SCREEN
34
KEYBOARD
30
CARD
READER
46
CLOCK

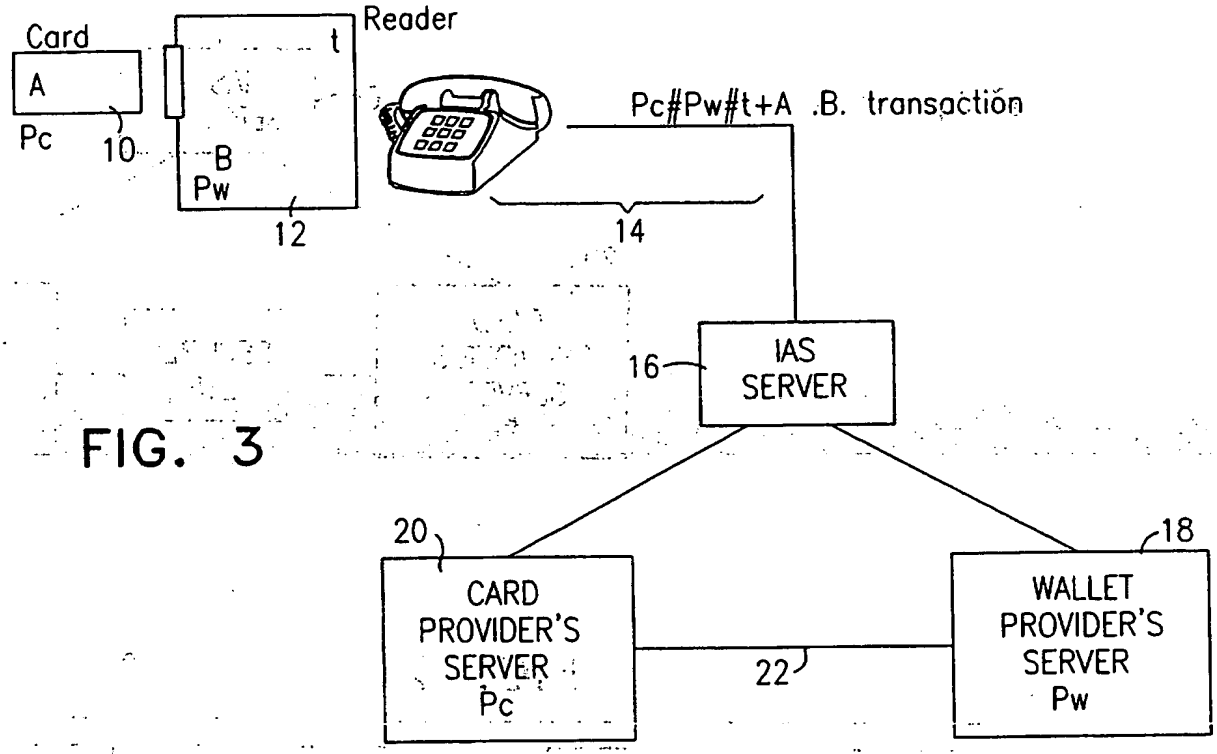


FIG. 3

FIG. 4

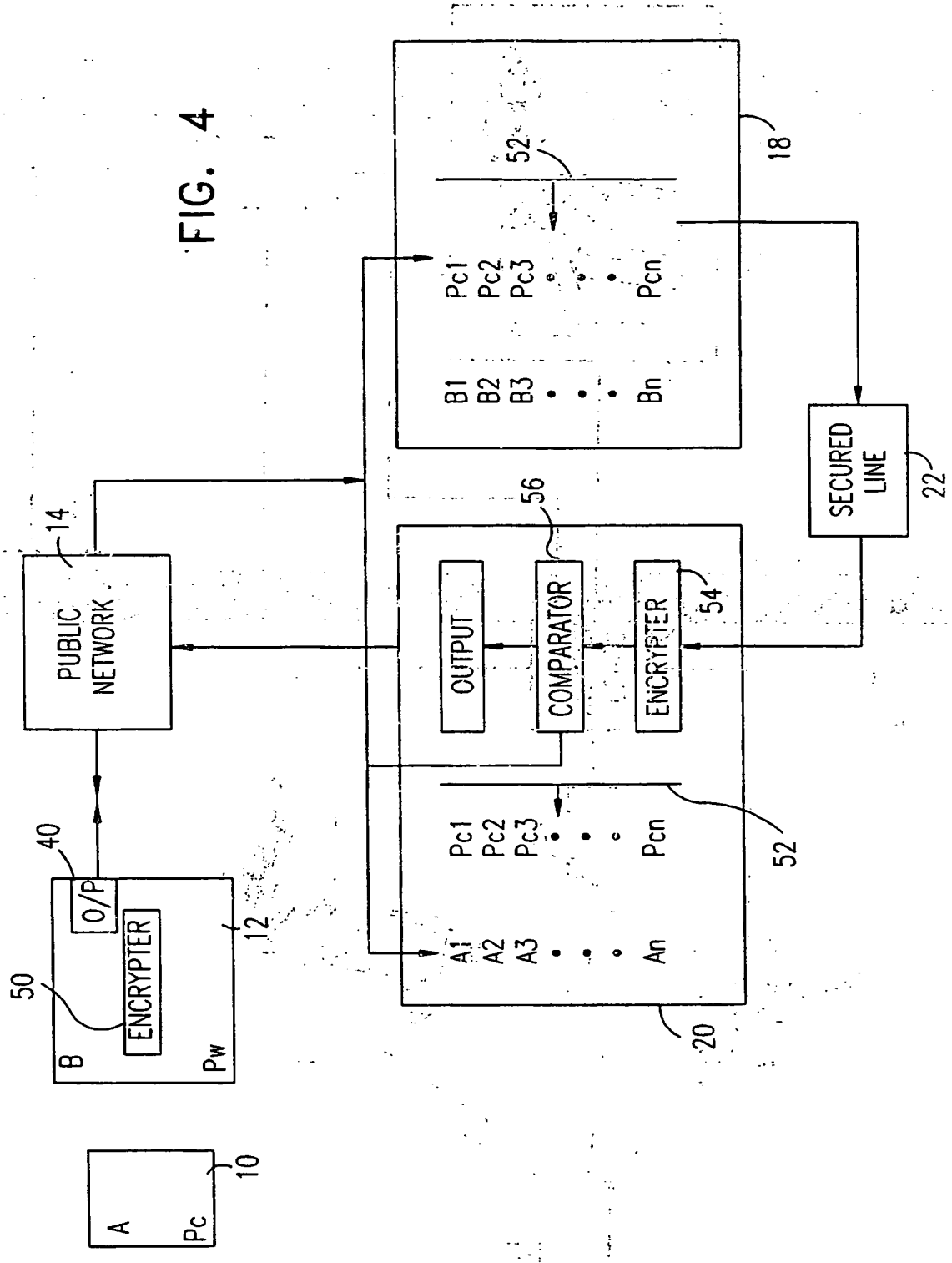
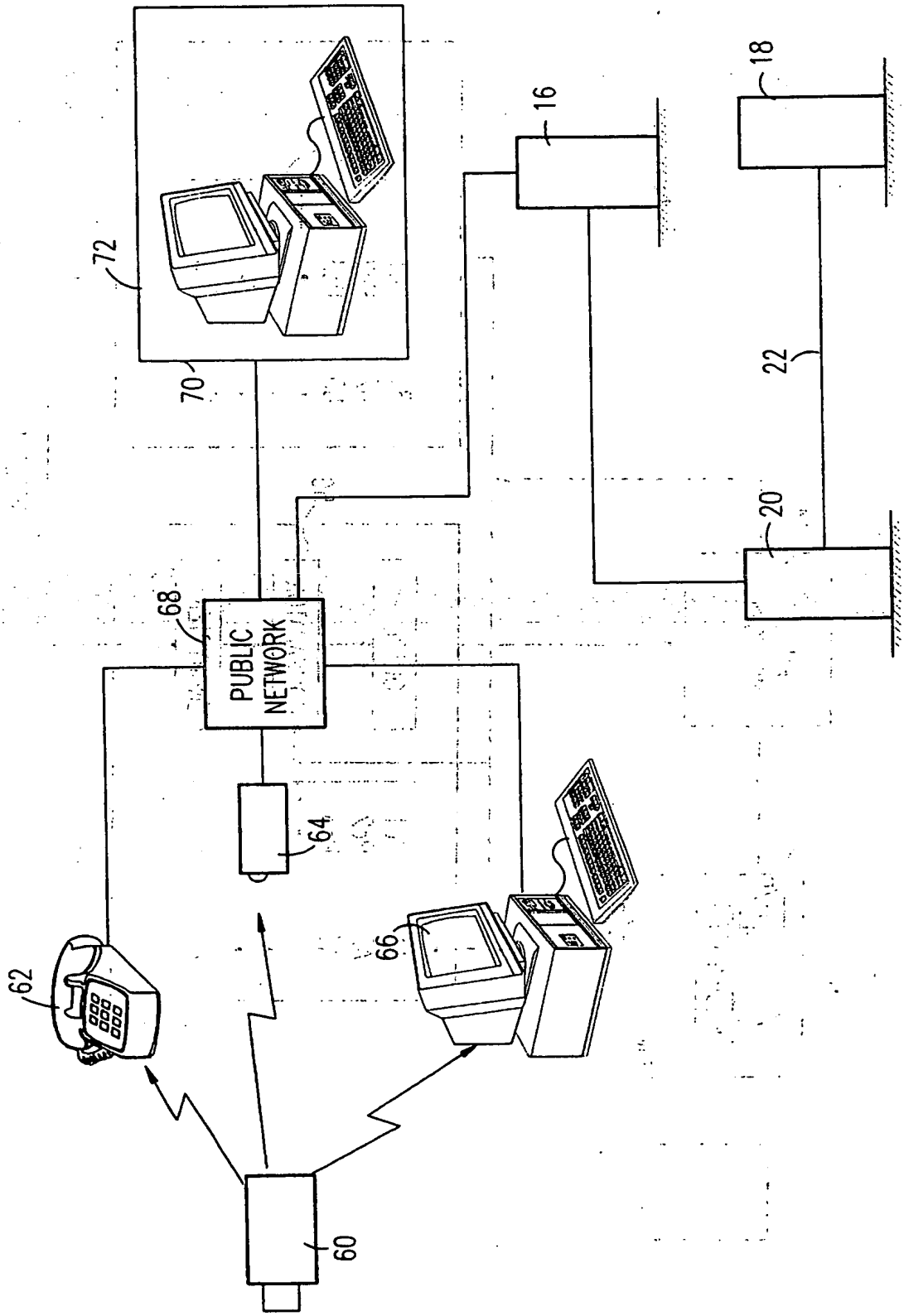


FIG. 5



INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL98/00116

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04K 1/00
US CL :380/23, 30, 49

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/23, 30, 49, 24, 25, 21, 4

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,379,344 A (LARSSON, et al.) 03 January 1995 (03.01.95).	1-12
A	US RE34,954 A (HABER, et al.) 30 May 1995 (30.05.95).	1-12
A	US 5,513,261 A (MAHER) 30 April 1996 (30.04.96).	1-12
A	US 5,534,857 A (LAING, et al.) 09 July 1996 (09.07.96).	1-12
A	US 5,592,553 A (GUSKI, et al.) 07 January 1997 (07.01.97).	1-12
A	US 5,623,637 A (JONES, et al.) 22 April 1997 (22.04.97).	1-12

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 02 JULY 1998	Date of mailing of the international search report 28 JUL 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer DAVID CAIN Diane Smith for Telephone No. (703) 305-1836

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL98/00116

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,694,471 A (CHEN, et al.) 02 December 1997 (02.12.97).	1-12
A, E	US 5,757,918 A (HOPKINS) 26 May 1998 (26.05.98).	1-12
A	US 5,347,580 A (MOLVA, et al.) 13 September 1994 (13.09.94).	1-12